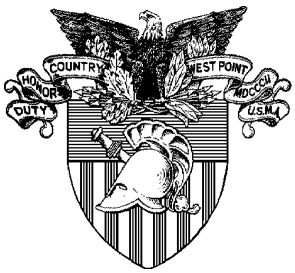


United States Military Academy

West Point, New York 10996

A Meta-Model Architecture for Fusing Battlefield Information

OPERATIONS RESEARCH CENTER OF EXCELLENCE
TECHNICAL REPORT DSE-TR-0517
DTIC #: ADA434915

Lead Analyst
Major Steven J. Henderson, M.S.

Senior Investigator
Patrick J. Driscoll, Ph.D.
Professor, Department of Systems Engineering

Approved by
Colonel Michael L. McGinnis, Ph.D.
Professor and Head, Department of Systems Engineering

May 2005

This research was generously sponsored by a grant from the Office of Force Transformation, Office of the Secretary of Defense, Washington, D.C.

A Meta-Model Architecture for Fusing Battlefield Information

OPERATIONS RESEARCH CENTER OF EXCELLENCE

TECHNICAL REPORT No: DSE-TR-0522

DTIC #: ADA434915

Lead Analyst
Major Steven J. Henderson, M.S.

Senior Investigator
Patrick J. Driscoll, Ph.D.
Professor, Department of Systems Engineering

Approved by
Colonel Michael L. McGinnis, Ph.D.
Professor and Head, Department of Systems Engineering

May 2005

This research was generously sponsored by a grant from the Office of Force Transformation, Office of the Secretary of Defense, Washington, D.C.

Abstract

The principal contributions of this study are four-fold. First, we propose and illustrate a unifying meta-model architecture for fusing information in sensor-based decision support systems capable of delivering to the user strong inference results in support of tactical decision-making. Second, we demonstrate the feasibility of a completely automated system performing effective estimation of force operational states based on sensor data alone using a new web-based interactive tactical simulation. Third, we show that this architecture can readily accommodate several major network inference methods that are designed to handle battlespace uncertainty. And lastly, we discuss how this approach can be used to directly assess the information advantage of US Forces relative to opposing force intelligence gathering capabilities and the implications of doing so on developing strategic deception operations.

Table of Contents

List of Figures

List of Tables

1. Introduction

The principal contributions of this study are four-fold. First, we propose and illustrate a unifying meta-model architecture for fusing information in sensor-based decision support systems capable of delivering to the user strong inference results in support of tactical decision-making. Second, we demonstrate the feasibility of a completely automated system performing effective estimation of force operational states based on sensor data alone using a new web-based interactive tactical simulation. Third, we show that this architecture can readily accommodate several major network inference methods that are designed to handle battlespace uncertainty. And lastly, we discuss how this approach can be used to directly assess the information advantage of US Forces relative to opposing force intelligence gathering capabilities and the implications of doing so on developing strategic deception operations..

Battlefield sensing technologies and techniques have become increasingly important in the transformed Army of the twenty-first century. Commanders seek to leverage information to gain unsurpassed battlefield dominance while at the same time reducing overall operational risk to soldiers in a variety of deployment scenarios [1, 2]. Our study responds directly to these priorities.

The underlying purpose here should be to enhance a commander's ability to perform effective inference concerning opposing force operational states because doing so leads to a natural notion of information advantage: friendly forces know more about what opposing forces are actually doing a significant period of time before the opposing force knows what friendly forces are doing. A simply constructed yet logically robust framework for performing this inference needs to avoid undue complexity, both in terms of logical structure (for implementation's sake) and raw information requirements (to avoid information overload). For sensor-based systems in particular, information overload becomes a concern if the end user is no longer able to productively use the quantity of information within the time scale available [15].

While new approaches to sensor data handling have been proposed to satisfy some of the performance demands of decision support systems [3, 4], tacit to such approaches is a design assumption that the quality of the information in such systems increases as the data

sample size generated by battlefield sensors increases in both quantity and dimensional representation. This assumption is based on the concept of *enumerative* logic, which accepts that evidence in support of a specific inference is accumulated over time and more evidence accumulated over time enhances the strength of this information with respect to this inference [6]. Exclusively adopting this philosophy naturally leads engineers to design and field increasingly complex battlefield networks capable of gathering, storing, and processing this information much faster than it can be understood and exploited by human decision makers [14].

To avoid information overload one could adopt a philosophy consistent with economic theory. This viewpoint contends that decision relevant information that does not alter a pre-existing decision is not information; it is only serves to confirm the decision that has been made [6]. We discourage such a parochial philosophy in a tactical setting because it fails to recognize the contribution that different forms of information make to a military decision-making. For example, there is tangible military value in conflicting, contradictory, and confirmatory information processed in support of verifying military targeting. These types of information typically arise as ancillary evidence, that is, evidence concerning evidence that goes to subjective concerns of credibility and believability on the part of users. To put it another way, information of this nature, while not information in the technical economic sense described above, nevertheless serves the vital military purpose of validating operational decisions. This kind of information strengthens rather than diminishing the inferential force of existing evidence. On a practical level, it strengthens the resolve behind command decisions.

In contrast to enumerative logic, *eliminative* logic provides a philosophical basis for supporting inference by seeking contradictory evidence that can negate alternative explanations. It is this logic that underscores the well-known practice of disproving conjectures by identifying counter-examples. Taken at its extreme, eliminative logic supports a conjecture that when all other possibilities have been eliminated, the remaining possibility condition is true. The culling nature of this philosophy has real potential to limit the occurrence of information overload.

It should be possible to combine both forms of logic: enumerative and eliminative, within the logical design of a fusion approach, much in the same way that primal-dual

approaches are used in mathematical programming [9] and game theory, playing against each other until some predetermined condition is satisfied. This strategy could exploit some portion of the in-flow buildup of real time opportunistic information yet limit the extent of overload by simultaneously imposing criteria that could appropriately cull the number of possible inference estimates the evidence gathered might reasonably support.

In this paper, we define and test a logical framework within which such a fusion approach could succeed. Figure 1 illustrates the placement of this study within a spectrum of possible systems modeling approaches [35]. While the meta-model architecture stands alone as a mechanism for illuminating a new perspective on intelligent systems design, it also advocates a general decision support tool that could be integrated in some fashion into a common operating picture (COP) for developing situational awareness of enemy operational state. Therefore, the study resides approximately midway between routine decision support and representing possible system design and changes in Figure 1.

This framework, called a *meta-model architecture*, incorporates the structural concept of a sensor network as an information manufacturing system [10] focused on estimating enemy intent through the surrogate of identifying the current enemy operational state. Doing so necessitates that we decompose and identify the layers of inference abstraction required to make such an identification, which we do in Section 2. This perspective sets apart our meta-model from other data fusion approaches such as that developed by the Data Fusion Subpanel of the Technology Panel for C3 (command, control, communications) of the Joint Directors of Laboratories (JDL) [16].

In Section 3, we formally introduce a meta-model architecture in the spirit of Wand and Weber [5] that simplifies the representation of information flowing in a sensor-based decision support system. Recognizing that such a framework must naturally accommodate the inherent uncertainty present in battlefield information, we demonstrate in Section 4 the meta-model's ability to accept three major stochastic network inference models: Bayesian Belief Network [19], Fuzzy Logic [20], and Probabilistic Modal Logic [21].

To illustrate the feasibility of this approach, we use results of recent computational experiment in which a new interactive web-based simulation identified a force's operational state by detecting the physical characteristics of force behavior. Following this, in Section 5 we discuss how this approach leads directly to a natural way of determining the information

advantage of US Forces relative to opposing force capabilities, concluding with comments in Section 6 pertaining to continued research in this area.

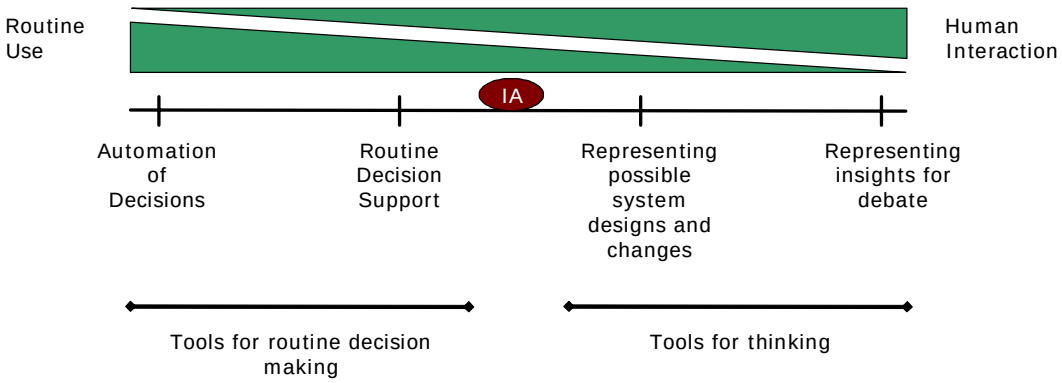


Figure 1. Placement of this study amidst a spectrum of systems modeling approaches.

2. Inference Structure

The layers of inference that must be negotiated in order to estimate operational intent increase as one examines the structure of battlefield information in finer granularity. Here, we limit our excursion in this regard to the simplest abstraction sufficient to illustrate both our motivation for and the challenges associated with identifying a force's operational state as a surrogate for intent. Figure 2 illustrates the inference structure underlying our meta-model approach. In the illustration, each of the vertical lines dividing the text boxes should be interpreted in the classic sense of "given" put forth in conditional logic.

This structure posits that intent provides the impetus for deciding a force's operational state. However, since intent is a pure intellectual construct it is not explicitly evident in the physical world. It must be communicated or transformed into action in order to become evident. In doing so, some elements of intent are lost when married to a force's

particular capabilities and resource constraints. Regardless, such a cognitive transformation results in an observable force operational state as an aggregate framework for action.

In concert with FM 3-0 [13], there are identifiable physical characteristics that enable one to distinguish between major force operational states. For example, the footprint of a force, its speed of movement, its massing or un-massing, the types of equipment present, and so on are all characteristics that bound what a force can accomplish, all other things being equal (e.g., motivation, morale). The proper structuring and control of these physical characteristics define tactics.

If we assume a rational decision process on the part of a force command, it follows that the major operational state selected from those available is one that best represents their intent conditioned by pragmatic compromises the command must make. Because true force intent is invisible to the observer, the observable characteristics of the chosen operational state serve as a necessary surrogate. This operational state defines physical actions taking place on the battlefield which are susceptible to detection, classification and identification by various types of sensor networks.

At the edge of these networks, sensors act as raw data generators, transforming physical indicators of presence and action into digital signals called sensor data. Rather than explicitly decomposing the elements of sensor data and sensor data uncertainty as in [18], we instead conceptualize the action of sensors as gathering evidence in support of or against various state characteristics, called *key descriptors*, further defined in Section 3. It is these key descriptors that allow one to distinguish between operational states.

At the key descriptor level, the inference layers bifurcate into two major paths defined by the sensor network purpose. Presumably, targeting networks would require threshold levels for individual elements of each key descriptor set to be met as conditions of acceptance. The composite perspective of each set then provides a targeting profile that supports engagement criteria, target identification, ordinance requirements, and supplemental actions required. On the other hand, and consistent with the focus of this paper, the key descriptor levels also support situational battlespace awareness. Along this path, such levels facilitate prediction of an enemy operational state which logically acts as a surrogate for creating estimates of enemy intent as well.

Even in this much simplified inference pathway from true intent to estimated intent, one gains a sense of the many layers of inference abstraction being negotiated in the process of using sensor data to produce estimates. The uncertainty introduced during each of the various transformations affecting an inferential transition between layers compounds the challenge. Hence, one can certainly understand the belief that 'more must be better,' an axiom of enumerative logic that leads to extensive information requirements for battlefield sensor networks.

By contrast, in the meta-model construction that follows, we aimed to minimize information requirements. Instead, we built an architecture predicated on the concept of gathering supporting data in an enumerative fashion and exploiting eliminative evidence in order to winnow the possible set of operational states. We relegate to the three probabilistic network learning models discussed in section 4 the task of dealing effectively with the underlying uncertainty present in such an approach.

3. Information Meta-model Architecture

In order to specify the information that a sensor-based system should acquire, it is necessary to first define and organize battlefield information in consideration of what is to be done with the information once it is obtained. Here, we introduce a set of ontological constructs and rules for defining and deriving battlefield information in support of an information fusion process. We use the term 'ontology' in the sense defined by Poli [17]: a theory of items and how to logically relate them. This is a categorical viewpoint that seeks to identify and structure universal items present in the domain of battlefield sensor networks and information.

This meta-model architecture affords a unifying framework that achieves several objectives. First, it operates under the condition that information available for inference will be limited. Second, it provides a fundamental definition of battlefield information that is directly coupled to estimating and predicting force operational state from low level sensor data. Third, it can accommodate multiple and diverse sensor technologies as a result of focusing on the information conveyed and not the technology used to convey it. Fourth, as demonstrated in the computational testing section later in this paper, it nicely accommodates several of the major network learning models used to accommodate inference under

uncertainty. And lastly, as we discuss later in the paper, it provides an effective operational definition for information advantage that can both guide future system development and supply a recipe for appropriate deception operations to complement major force operational states.

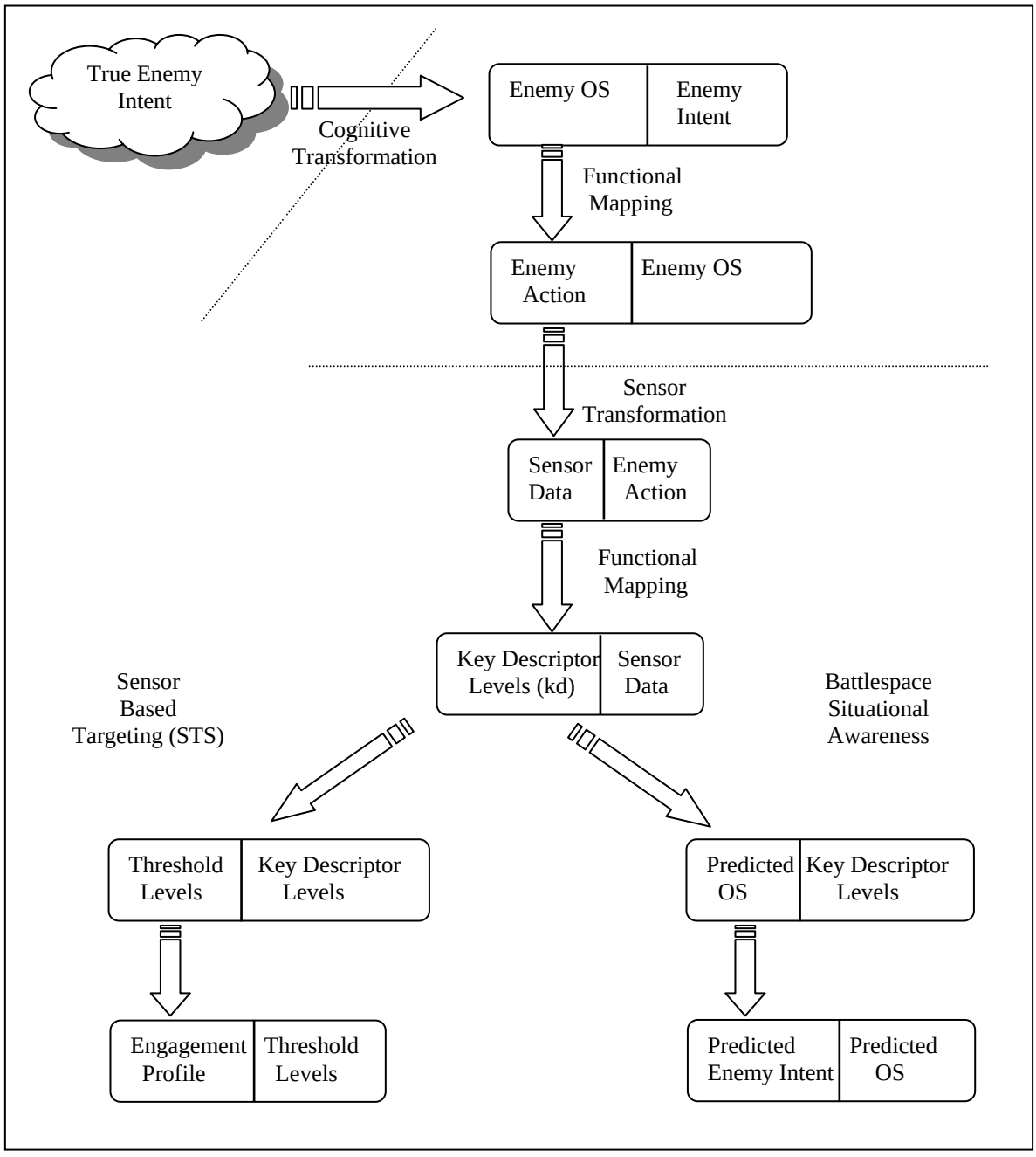


Figure 2. Abstraction layers for estimating enemy intent using sensor networks.

By assuming that intent provides a complete and sufficient motivation for force action in a battlespace environment, we impose the condition that a body of force acts as a (possibly loosely) coordinated organization. The totality of actions motivated by force intent define an *operational state*. An operational state ultimately represents evidence supporting an underlying operational intent while intermingled with intentioned deception and operational errors. Since battlefield sensors cannot discriminate between these elements, it seems reasonable to expect the structure of any battlefield information framework to somehow process all three in such a way that the actual operational state eventually becomes predominant. We assume that deception and operational errors represent a minority propotion of the total evidence present on the battlefield based on the principles of warfare discussed in FM 3-0. FM 3-0 also supports our assumption that, excepting minor variations in theme, the major number of independent (possibly unique) operational states a particular force is able to assume in a known battlespace is finite.

3.1. Model structure

The meta-model, *M*, we propose is concisely defined by a 5-tuple *M*= (S, V, K, O, E) that captures the necessary elements of the battlespace we need to identify operational state. Figure 3 shows a graphical illustration of the entity arrangement that follows. In the ontological framework proposed by Wand and Weber [5], *M* corresponds to a *modeling grammar*. In the following paragraphs, we define each member of this tuple using standard notation suggested by Wymore [22]. The underlying inference logic connecting each of the elements of information within this structure is Pascalian, meaning that support for or against a particular hypothesis concerning activity is accumulated over time.

Let S represent a finite set of *m sensors*, $S = \{s_1, s_2, \ldots, s_m\}$. Here we refer to sensors in the generic sense allowing for the inclusion of human and other sources capable of generating battlespace information products. Each of these sensors performs a constrained functional transformation of activity in the physical world to various information products. These products can span a host of mediums and forms ranging from simple items of primitive data to complex ones such as summary reports constructed by multimode, multi-process sensor networks. As such, let V represent a finite collection of *n* possible sensor

information product *values*, $V = \{v_1, v_2,..,v_n\}$, where sensor s_m assuming the value v_n is denoted by $s_m(v_n)$.

Let K represent a finite set of *q key descriptors*, $K= \{kd_1, kd_2, \ldots, kd_q\}$. Each key descriptor acts as a discriminant function $kd_i = \{ (x, p) : x = s_m(v_n) \subseteq S \times V, \ p \in R \ \}$ by mapping subsets of feasible sensor-value pairs $s_m(v_n)$ to a support value, *p*. Each real value *p* represents a certainty metric associated with the truth-value of a particular key descriptor based on the presence of its associated sensor values. We intentionally define *p* over the entire set of real numbers R to accommodate various forms of uncertainty modeling. Specific implementations of this meta-model will most likely restrict *p* to a certain subset of R, as is the case with Kolmogorov probability measures [15] that limit the range of probability to 0 to 1.

Let O represent a finite set of *t* mutually exclusive *operational states*, $O = \{o_1, o_2, \ldots, o_t\}$. Each operational state characterizes a distinct, organized, major force action whose motivation is supplied by force intent. Each operational state is of the form $o_i = \{ (y, p) : y \subseteq K, \ , \ p \in R \ \}$,
and maps subsets of key descriptor values to a final level of support value *p* in R . The value *p* represents the certainty associated with the truth-value of an operational state.

E represents an operational state *estimation* function, $E = \{ (z, e) \ : \ z \subseteq O, \ e = \{ e_1, e_2, \ldots, e_t\}, e_i \in R\}$ in which each value e_i corresponds to the overall certainty of an operational state o_i when evaluated in the context of *all operational states*. This function is necessary for obtaining meaningful fusion results as one or more operational states may individually incur competing certainty values. The estimation function provides flexibility in defining how each operational state's certainty is interpreted with respect to other operational states' certainty. For example, if the risk posed to friendly force for a particular operational state is high, then even a small level of certainty for that operational state may be more significant than a high level of certainty from a lower risk operational state.

The definitions for K, O, and E represent the main mechanisms for data fusion in our model and are deliberately defined in general terms to enhance the meta-model's applicability to a wide range of underlying fusion techniques. This generalization avoids over-constraining how one defines either the mapping of sensors to key descriptors and key descriptors to operational states so that the meta-model can readily accept the wide variety of

such mappings offered by major network inference methods designed to deal with uncertainty.

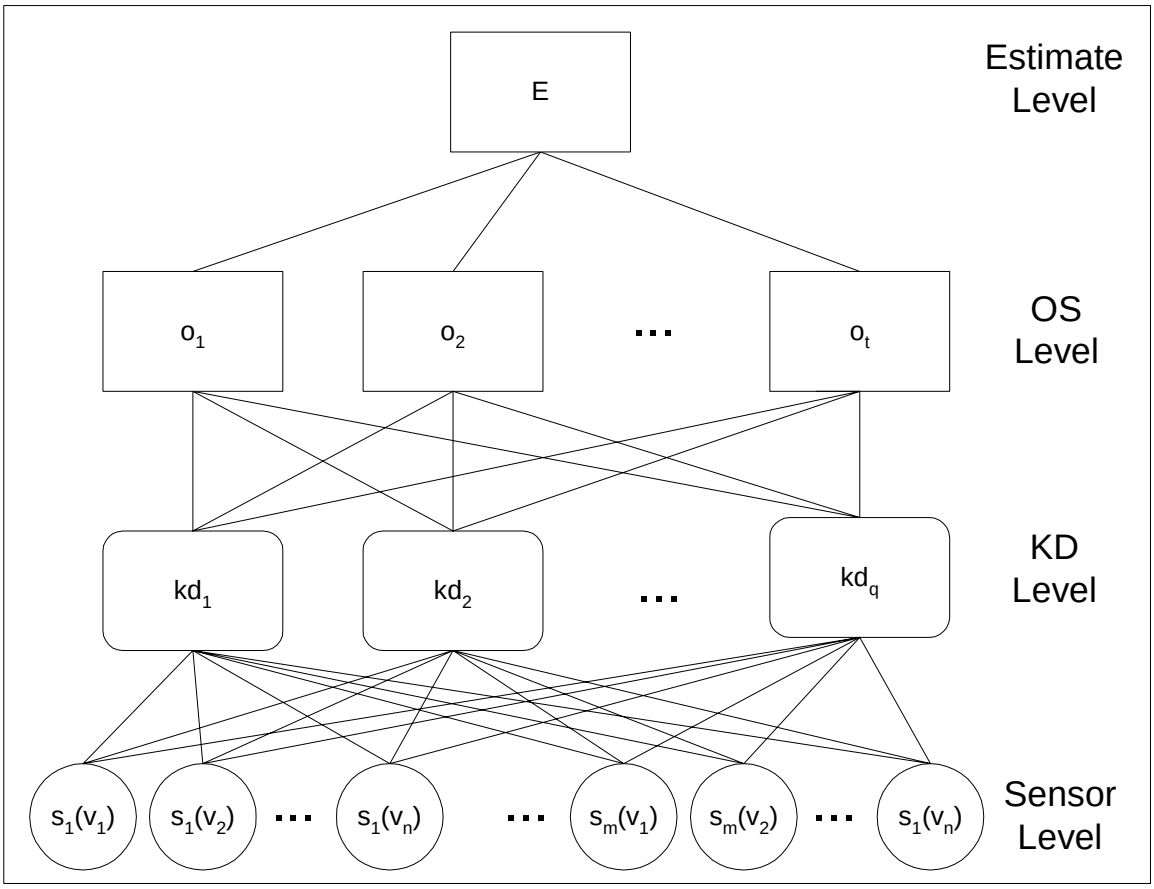


Figure 3. Entity arrangement of the information meta-model.

Lastly, to avoid unnecessary complications at this stage of inquiry we chose to exempt explicit time factors from the various functional mappings used in our architecture. A straightforward modification of either estimation functions or key descriptor mappings can easily incorporate time effects such as the value of tactical information [25], or on the timeliness of data within the network flow [23], if such factors were of direct interest.

The following examples illustrate how one employs this architecture to capture various information elements necessary to support effective inference concerning force operational state.

3.1.1. Example Model 1

Let M_1 = (S, V, K, O, E) and define each of the elements of M as follows: S = {$Acoustic_1$, $Soldier_1$, $Radar_1$, $Acoustic_2$, $Soldier_2$, $Radar_2$}.

Here, a sensor type and an index distinguish each sensor. To clarify, $Acoustic_1$ indicates the first sensor in the class of acoustic sensors. In this example, the sensors with subscripts equal to one are located on the west side of a hypothetical battlefield while the sensors with subscript equal to two are located on the east side of the battlefield.

$V = \{v_{acoustic} \cup v_{soldier} \cup v_{radar}$:

$v_{soldier}$ ={tank, truck, aircraft, artillery_impact}

$v_{acoustic}$ = {vehicle, aircraft, explosion}

v_{radar} = {friendly, enemy, unknown }}

The domain of all possible sensor values is defined in terms of the possible values for each sensor type.

K = {{kd_1, kd_2, kd_3, kd_4} :

kd_1 = ((x, p) : x = { ($Soldier_1(a_1)$, $Acoustic_1(a_2)$ } ,
$p \in$ RLS[-1, 1];
if a_1 = tank and a_2 = vehicle then p = 1.0,
else p = 0.0),

kd_2 = ((x, p) : x = { ($Soldier_2(a_1)$, $Acoustic_2(a_2)$ } ,
$p \in$ RLS[-1, 1];
if a_1 = tank and a_2 = vehicle then p = 1.0,
else p = 0.0),

kd_3 = ((x, p) : x = { $Radar_1(a_1)$ } , p $\in$ RLS[-1, 1];
if a_1 = enemy then p = 1.0,
else p = 0.0)

kd_4 = ((x, p) : x = { $Radar_4(a_1)$ } , $p \in$ RLS[-1, 1];
if a_1 = enemy then p = 1.0,
else p = 0.0)}

For this example, we define each key descriptor as a predicate logic formula that maps a subset of sensor-value pairs to *a certainty factor* measure adapted from that used in the MYCIN expert system [24]. A certainty factor of 1.0 represents absolute certainty that the key descriptor is true or present. A certainty factor of –1.0 represents absolute certainty that the key descriptor is false, or not present. A value of 0.0 represents complete uncertainty. In this sense, the specific implementation of each function kd_i is similar to rules used in a knowledge base or expert system.

$O = \{ \{o_1 , o_2\}:$

$o_1 = ((x, p) : x = \{kd_1, kd_3\} , p \in RLS[-1, 1];$
if (kd_1=1.0) and (kd_3=1.0) then p = 1.0,
else p = 0.0)

$o_2 = ((x, p) : x = \{kd_2, kd_4\} , p \in RLS[-1, 1];$
if (kd_2=1.0) and (kd_4=1.0) then p = 1.0,
else p = 0.0)}

To enhance readability we can optionally assign meaningful terms to each operational state such as: o_1 = attack_east, o_2 = attack_west . We again define our functions as a series of predicate logic formulas and restrict values of p to represent a certainty factor.

Finally, define the estimate function as a normalization of each state's certainty factor as:

$$E = \{(x, (e_1, e_2)) : x = \{o_1, o_2\}; e_i = o_i / (o_1 + o_2) \text{ for } i = \{1, 2\}\}$$

Figure 4 depicts a graphical version of the model for this example. To fuse information with this meta-model, suppose that each of our sensors generates the following information:

$Soldier_1$(tank), $Soldier_2$(truck), $Acoustic_1$(vehicle)
$Acoustic_2$(vehicle), $Radar_1$(enemy), $Radar_2$(unknown)

Calculating the values of key descriptors yields: $\{ kd_1, kd_2, kd_3, kd_4 \} = \{1.0, 0.0, 1.0, 0.0\}$. These in turn produce the operational state values: $\{o_1, o_2\} = \{1.0, 0.0\}$. From this result, we apply the estimation function and derive the following overall estimates for e_1, and e_2: {1.0, 0.0}. From these estimates, we infer that most likely enemy operational state is o_1, or attack_west.

3.1.2. Example Model 2

While Example 1 serves to illustrate the basic mechanics of the meta-model, it does not address one of the major difficulties in information fusion – uncertainty. Model M_1's minimal set of sensors that defines each key descriptor is mutually exclusive. Likewise, the minimal set of key descriptors that defines each operational state is also mutually exclusive. Under these conditions, identifying the enemy's operational state is a relatively simple matter of detecting what is and is not present on the battlefield. More interesting is the case where such sets possess elements that are not mutually exclusive – *e.g*. one or more sensors provides information in support or against more than one key descriptor, or one or more key descriptors provides information about one or more operational states. As Antony stresses [12], this type of uncertainty is a likely result of any fusion process:

> "Despite a more global perspective and the use of all the available sensor derived information, the nondeterministic nature of the domain, and the largely exception-based character of the reasoning process virtually assures that there will exist some degree of uncertainty in the fusion product."

This second example provides a more complicated scenario that demonstrates how the meta-model can accommodate such uncertainty. Figures 5, 6, and 7 show several "cartoon sketches" that best introduce the example. We now formally introduce the model, M_2:

$O = \{o_1 = \text{withdraw}, o_2 = \text{defend}, o_3 = \text{west\_attack}, o_4 = \text{east\_attack}, o_5 = \text{dual\_attack}\}$

$S = \{S_1, S_2, S_3, S_4, S_5, S_6\}$

$V = \{\text{tank}, \text{fuel\_truck}, \text{recon\_vehicle}\}$

For ease of readability, we replace the mathematical definition of key descriptors with the following compact definition:

$$(S_1 = x, S_2 = x, \ldots, S_n = x_n) \Rightarrow \text{pr}(KD_i) = p$$

This definition states that if each listed sensor value has the specified value, then KD_i adopts a degree of certainty *p* (and adopts a value of zero otherwise). We now define our key descriptors using this notation:

$$
\begin{aligned}
K = \{&(S_1 = \text{tank}, S_2 = \text{fuel\_truck}) \Rightarrow pr(KD_1) = 1.0 \\
&(S_i = \varnothing \ \forall\ i = \{3,..,7\}) \Rightarrow pr(KD_2) = 1.0 \\
&(S_2 = \text{tank}, S_3 = \text{recon\_vehicle}, S_4 = \text{recon\_vehicle}) \Rightarrow pr(KD_3) = 1.0 \\
&(S_i \neq \text{tank} \ \forall\ i = \{5,6,7\}) \Rightarrow pr(KD_4) = 1.0 \\
&(S_3 = \text{tank}, S_6 = \text{tank}) \Rightarrow pr(KD_5) = 1.0 \\
&(S_i \neq \text{tank} \ \forall\ i = \{5,7\}) \Rightarrow pr(KD_6) = 1.0 \\
&(S_4 = \text{tank}, S_7 = \text{tank}) \Rightarrow pr(KD_7) = 1.0 \\
&(S_i \neq \text{tank} \ \forall\ i = \{5,6\}) \Rightarrow pr(KD_8) = 1.0 \\
&(S_3 = \text{tank}, S_5 \neq \text{tank}, S_6 = \text{tank}) \Rightarrow pr(KD_9) = 1.0 \\
&(S_4 = \text{tank}, S_5 \neq \text{tank}, S_7 = \text{tank}) \Rightarrow pr(KD_{10}) = 1.0 \\
&(S_i = \text{tank} \ \forall\ i = \{3,4,5\}) \Rightarrow pr(KD_{11}) = 1.0 \\
&(S_6 = \text{recon\_vehicle}, S_7 = \text{recon\_vehicle}) \Rightarrow pr(KD_{12}) = 1.0 \\
&(S_3 = \text{tank}, S_4 = \text{tank}) \Rightarrow pr(KD_{13}) = 1.0\}
\end{aligned}
$$

We use the same compact form to specify our operational states:

$$
\begin{aligned}
O = \{ &(kd_1 = 1.0,\ kd_2 = 1.0) \Rightarrow pr(\text{withdraw}) = 1.0 && (r_1) \\
&(kd_3 = 1.0, kd_4 = 1.0) \Rightarrow pr(\text{defend}) = 1.0 && (r_2) \\
&(kd_5 = 1.0, kd_6 = 1.0) \Rightarrow pr(\text{west\_attack}) = 1.0 && (r_3) \\
&(kd_7 = 1.0, kd_8 = 1.0) \Rightarrow pr(\text{east\_attack}) = 1.0 && (r_4) \\
&(kd_9 = 1.0, kd_{10} = 1.0) \Rightarrow pr(\text{dual\_attack}) = 1.0 && (r_5)
\end{aligned}
$$

Each of the first five rules for operational states exclusively define one particular state. The key descriptors in these rules do not appear in any other rules. We now define several additional rules containing key descriptors that provide supporting information to more than one operational state:

$(kd_{11}=1.0) \Rightarrow \text{pr(dual\_attack)} = 0.5$ (r_6)

$(kd_{11}=1.0) \Rightarrow \text{pr(west\_attack)} = 0.5$ (r_7)

$(kd_{11}=1.0) \Rightarrow \text{pr(east\_attack)} = 0.5$ (r_8)

$(kd_{12}=1.0) \Rightarrow \text{pr(defend)} = 0.1$ (r_9)

$(kd_{12}=1.0) \Rightarrow \text{pr(west\_attack)} = 0.3$ (r_{10})

$(kd_{12}=1.0) \Rightarrow \text{pr(east\_attack)} = 0.3$ (r_{11})

$(kd_{12}=1.0) \Rightarrow \text{pr(dual\_attack)} = 0.3$ (r_{12})

$(kd_{13}=1.0) \Rightarrow \text{pr(dual\_attack)} = 0.33$ (r_{13})

$(kd_{13}=1.0) \Rightarrow \text{pr(west\_attack)} = 0.33$ (r_{14})

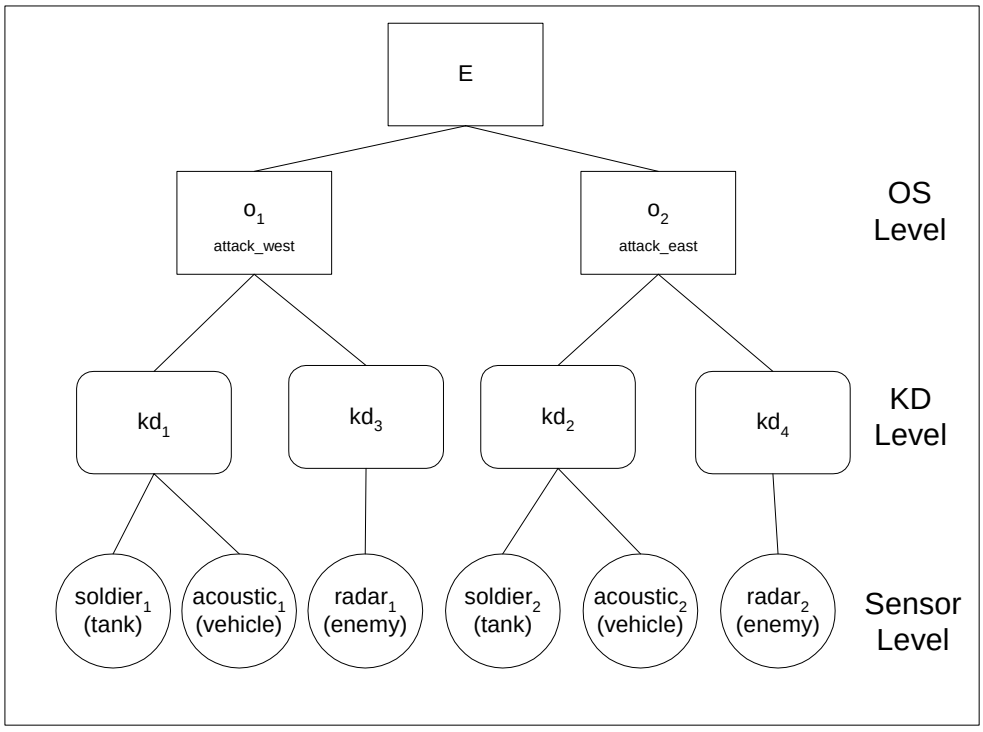


Figure 4 – Graphical Depiction of Example Model M_1

$(kd_{13}=1.0) \Rightarrow \text{pr(east\_attack)} = 0.33$ (r_{15})

$\text{pr}(o_k) = \text{pr}(o_k)|r_i + \text{pr}(o_k)|r_j -$

$\text{pr}(o_k)|r_i \times \text{pr}(o_k)|r_j \quad \forall\ k\ \}$ (r_{16})

The last element in O, (r_{16}), which commonly appears in expert systems such as MYCIN, is needed to resolve contradictory levels of support that might arise in the evaluation of r_1 - r_{15}. For example, when presented with KD_9, KD_{10}, and KD_{11}, rules r_5, r_6, r_7, and r_8 would all trigger. Two of these rules, r_5 and r_6, provide a contradictory certainty factor relevant to operational state o_5 (dual_attack). Rule r_5 yields a certainty factor of 1.0 while r_6 yields a certainty factor of 0.5. The estimation $e(o_5)$ assumes a different value depending on which rule triggered first. The formulation of r_{16} allows for the meaningful combination of all applicable values independent of sequential order of activation.

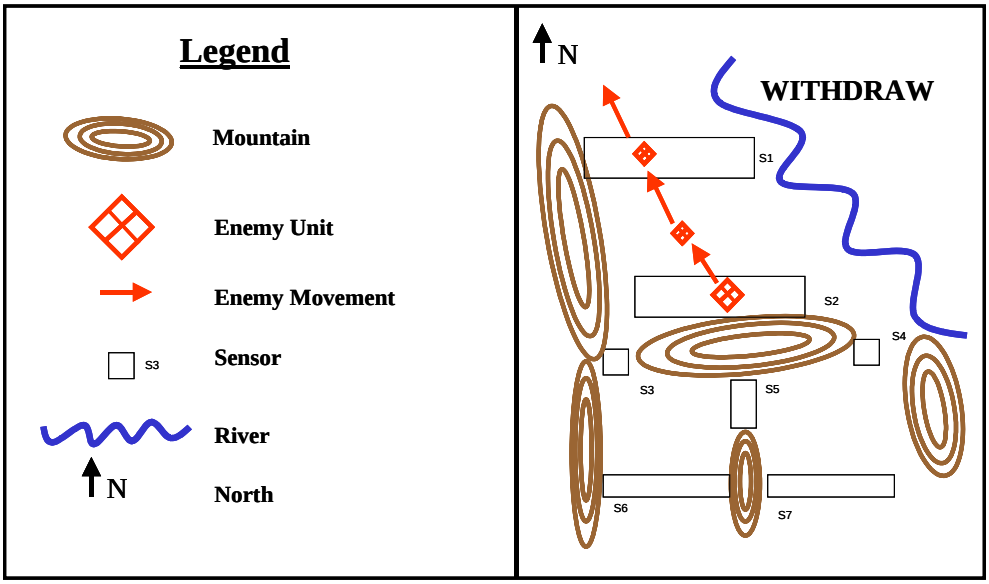


Figure 5. Example Model M_2 (Legend and Withdraw State)

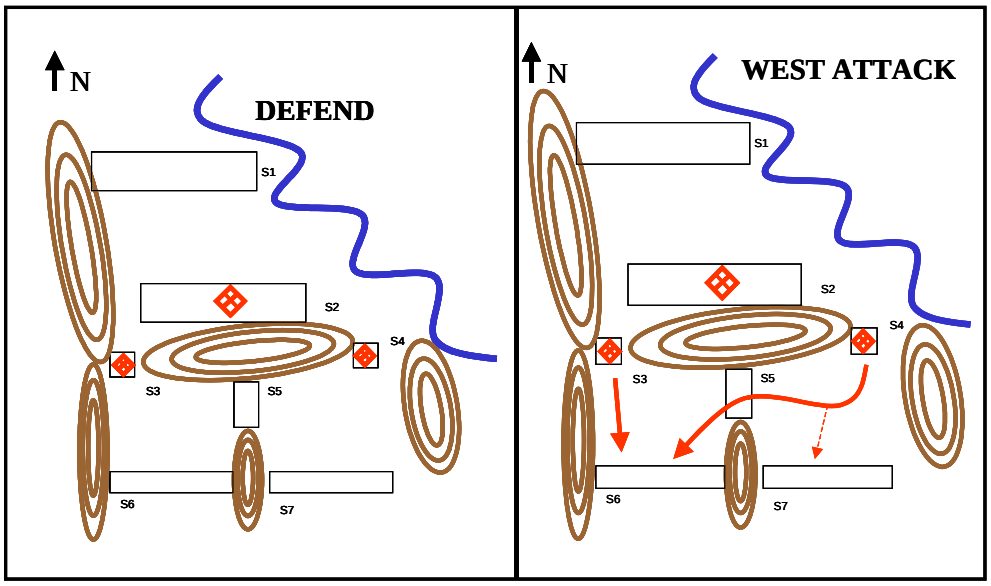


Figure 6. Example Model M_2 (Defend and West Attack States)

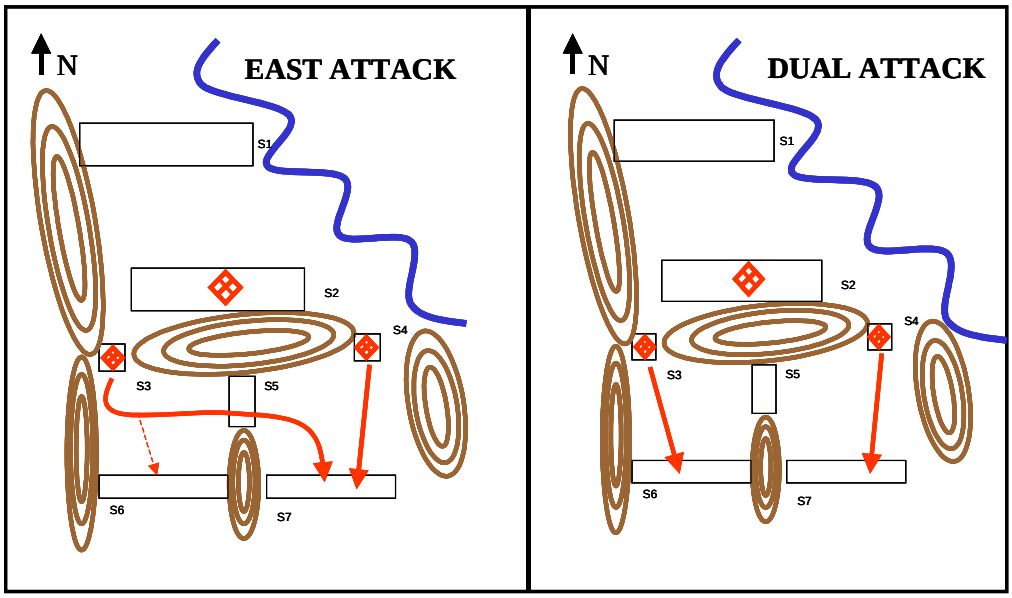


Figure 7. Example Model M_2 (East and Dual Attack States)

Finally, we define an estimator function as a normalizing function across all operational state values:

$$E = \{(x, (e_1, e_2, ..., e_5)) : x = \{o_1, o_2, \ldots, o_5\};$$

$$e_i = o_i / (o_1 + o_2 + o_3 + o_4 + o_5) \text{ for } i = \{1,2, .. , 5\}$$

When this model is presented with a piece of new information: S_2(tank), support is provided for $\{KD_2, KD_4, KD_6, KD_8\}$. However, these KDs do not activate any of the rules in O. Therefore, the following probabilities are assigned to each operational state:

$$pr(o_i) = 0.0 \; \forall \; i = \{1, \ldots,5\}$$

Suppose now that additional information becomes available: S_2(tank), S_3(recon_vehicle), S_4(recon_vehicle), which activate the set $\{KD_3, KD_4, KD_6, KD_8\}$.

This set of key descriptors uniquely satisfies r_2, so we update the certainty factor of o_2 (defend) to 1.0. Likewise, $pr(o_i) \; \forall \; i \neq 2$ remains at 0.0. Updating the values of E yields the following estimates (e_i) for each operational state – {0.0 , 1.0, 0.0, 0.0, 0.0 }. From this result, we deduce that the enemy's operational state is to defend.

Assuming that the battlefield situation continues to develop, suppose that new information is generated into the sensor network: S_2(tank), S_3(tank), S_4(tank), S_6(tank), S_7(recon_vehicle). These sensors, activate $\{KD_5, KD_6, KD_9, KD_{13}\}$, and this set of key descriptors satisfies rules r_3, r_{13}, r_{14}, and r_{15}. Note, our combining rule, r_{16} must be applied to resolve the conflict of r_3 and r_{14}. The resultant values for O are:

pr(withdraw) = 0.0

pr(defend) = 0.0

pr(west_attack) = 1.00

pr(east_attack) = 0.33

pr(dual_attack) = 0.33

Applying the estimation function E yields the following estimates for each operational state: {0, 0, 0.60, 0.20, 0.20}. From this result we deduce that o_5, or dual_attack, is the actual operational state.

4. Computational Experiments

As stated earlier in the paper, our interest in computational testing is two-fold: to examine how easily the major network inference models can exploit the meta-model framework, and to assess the quality of each of their resulting inferences concerning a force's actual operational state in the face of inherent uncertainty.

We designed a web-based computational experiment [11] involving three major network inference models. The experiment featured an interactive Java-based simulation of an unopposed force executing one of thirty-four possible missions. These missions, authored by individual human interaction with the simulation, reflected possible adaptations of one of five force operational states –Sustainment, Decisive Attack, Shaping Attack, Decisive Defense, and Shaping Defense [13]. Within this test environment, each participant had the ability to structure their force layout and movement in any way they desired so long as they arrayed these activities to achieve the assigned mission.

Once an operation was executed, a set of simulated sensors gathered evidence of low-level activity for several hundred enemy agents while continually updating a set of sixteen key descriptors. We forged these key descriptors during pre-experiment tuning by applying expert tactical knowledge to a set of test missions. For each mission, the three simultaneous implementations of the meta-model used these key descriptors to identify the actual enemy operational state. The following paragraphs briefly describe each implementation. While a full discussion and design specification for each of the network learning models is beyond the scope of this paper, it is available in [11] and can be supplied upon request of the authors.

The first network learning model implementation of the meta-model featured a Bayesian Belief Network (BBN) design. This implementation designates each of the five possible operational states as one of five hypotheses. Each hypothesis is assigned a preset prior probability based on the enemy's last known operational state, the initial prior being the usual naïve neutral. The design establishes conditional probabilities for each operational state-key descriptor pair reflecting the likelihood of each state given the presence of the key descriptor. Figure 8 illustrates a scaled-down, three hypotheses version of this design.

During simulation, the BBN implementation executes the following algorithm. As the enemy carries out his mission, the fusion coordinator updates key descriptor values based

on sensor detection of enemy agents. The fusion coordinator then computes a posterior probability by applying standard Bayesian updating methods [8] to the previously described BBN. Once the fusion coordinator obtains a certain threshold in posterior values (i.e. one operational state hypothesis dominates the others), a new set of priors is loaded and the algorithm repeated.

The second implementation featured a Probabilistic Modal Logic (PML) design largely championed by Halpern [7]. This design conceptualizes operational states as possible worlds – one world for each of the five possible operational states introduced previously. The PML relationship function between the possible worlds reflects the likelihood that, given the enemy's perceived operational state, the enemy is actually in another alternate operational state. We created these relationship functions based on the similarities of the five operational states to one another in both time and space dimensions. For each world, we designated a compact rule set that uses the support for specific key descriptors to reason about the enemy's next state.

The PML fusion algorithm functions similarly to the BBN algorithm. The fusion coordinator first establishes a perceived operational enemy state as the current world. The algorithm then updates key descriptor values based on simulation events, and uses these values to trigger the specific rule sets in the current world and all adjoining possible worlds. The algorithm then uses combined reasoning across all worlds to arrive at truth-values for the enemy's next state. Once one particular next state probability dominates, the fusion coordinator establishes a new current world and repeats the algorithm.

The third implementation used a Fuzzy Logic approach [20]. The design centers around thirty-two fuzzy logic rules. Each rule's antecedent includes one fuzzy variable for the current state, and one or more fuzzy variables for the key descriptor values. The rule consequents contain one or more variables for the next state. The current state and next state fuzzy variables contains five fuzzy sets, where each fuzzy set defines one possible operational state. Given an assumed operational state, the membership function for each of these five sets indicates how much each possible state in the universe of discourse satisfies the assumed operational state. This allows the model to capture the "likeness" of operational states that might be similar in time or space. For example, Figure 9 depicts a sustainment fuzzy set for the Current State and Next State fuzzy variables.

The Fuzzy Logic algorithm first establishes a value for the Current State fuzzy variable based on the enemy's last known operational state. The fusion coordinator then updates key descriptor fuzzy variables based on sensor perception of enemy agents inside the simulation. The fusion coordinator then evaluates each fuzzy rule, and uses Fuzzy Logic to combine the rule conclusions into a combined estimate about the enemy's next state. If one of these estimates exceeds the decision threshold, then the fusion coordinator updates the current state fuzzy variable and repeats the algorithm.

4.1. Computational Results

As previously mentioned, we used a portion of our original data to tune each meta-model implementation before opening the experiment to the test authors. This tuning phase involved simulating twenty-five missions (five randomly selected from each operational state) and modifying various parameters in each implementation (e.g. conditional probabilities in BBN, rule sets in PML, fuzzy membership functions in Fuzzy) until the implementations performed in an acceptable manner. We defined acceptable performance as an implementation's estimated operational state equal to the actual enemy operational state at simulation termination for all tuning missions.

Following this tuning, thirty-four new missions were introduced by various authors, each from one of the various five operational states. We again note that authors were completely free

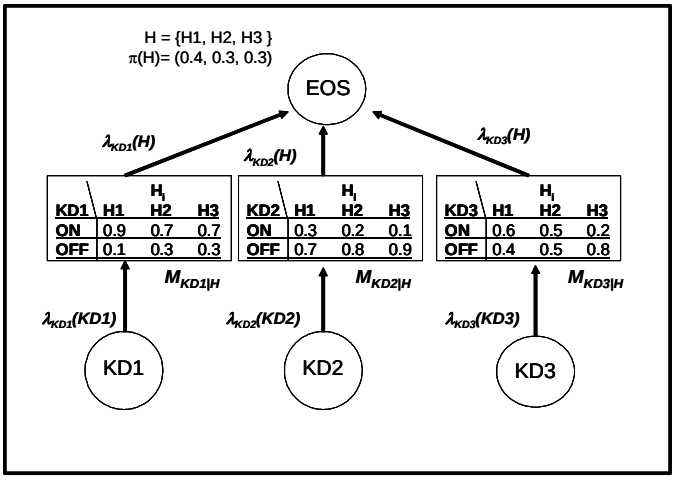


Figure 8. Meta-model BBN implementation.

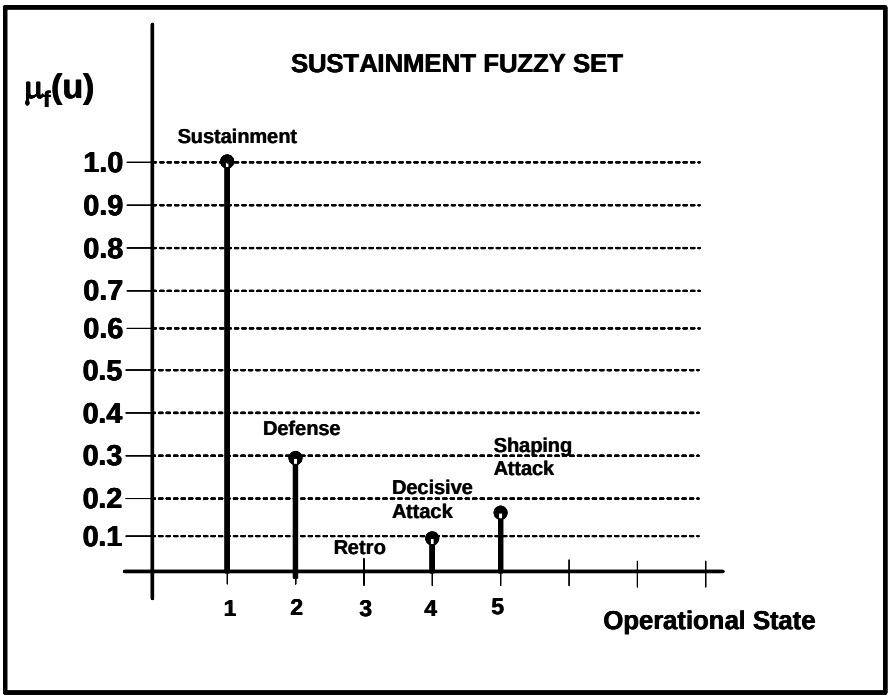


Figure 9. Sustainment fuzzy set used for meta-model implementation.

to position their forces and their movement in any way desired, no matter how unorthodox their choice, as long as it was consistent with achieving the mission. Our desire was to not constrain the boundaries of the operational state space any more than absolutely necessary so that we adequately stressed the meta-model framework.

	MISSION #	BBN	PML	FUZZY
SUSTAIN	#2329	0	0	0
	#9473	0	0	0
	#1010	0	0	0
	#5100	0	0	0
	#7338	0	0	0
	#7306	0	0	0
DEFENSE	#0285	0	0	0
	#6018	0	0	0
	#6463	0	0	0
	#4263	0	0	0
	#2772	0	0	0
	#5265	0	0	0
	#4007	0	0	0
	#4402	0	0	0
	#7581	0	0	0
	#0179	0	0	0
RETRO	#2990	0	0	0
	#1301	0	0	0
	#1746	0	0	0
	#6087	0	0	0
	#5995	0	0	0
	#7446	0	0	0
	#6312	0	0	0
D_ATK	#9026	1	1	1
	#7733	0	0	0
	#2775	0	0	0
	#7266	0	0	0
	#5412	1	1	01
	#3668	0	0	0
S_ATK	#0810	1	1	1
	#9437	0	0	0
	#8069	0	0	0
	#8214	0	0	0
	#9360	0	0	0

Table 1. PM4 results.

	MISSION #	BBN	PML	FUZZY
SUSTAIN	#2329	0	0	0
	#9473	0	0	0
	#1010	0	0	0
	#5100	0	0	0
	#7338	0	0	0
	#7306	0	0	0
DEFENSE	#0285	0.0889	0.0889	0.037
	#6018	0.0343	0.0343	0.0294
	#6463	0.049	0.049	0.0455
	#4263	0.1213	0.1011	0.1169
	#2772	0.254	0.254	0.1111
	#5265	0.2761	0.2761	0.2515
	#4007	0.0482	0.0482	0.0442
	#4402	0.2117	0.2117	0.1892
	#7581	0.1416	0.1416	0.2124
	#0179	0.1767	0.1767	0.1729
RETRO	#2990	0.1692	0.1662	0.8852
	#1301	0.1232	0.1327	0.6351
	#1746	0.0814	0.2073	0.601
	#6087	0.0389	0.0389	0.6721
	#5995	0.4405	0.4277	0.8103
	#7446	0.4751	0.9669	0.4807
	#6312	0.8157	0.959	0.9556
D_ATK	#9026	1	1	1
	#7733	0.053	0.0436	0.0398
	#2775	0.381	0.381	0.381
	#7266	0.2584	0.2584	0.2472
	#5412	0.9669	1	0.5626
	#3668	0.2491	0.4555	0.3701
S_ATK	#0810	1	1	1
	#9437	0.1741	0.1741	1
	#8069	0.3261	1	0.3435
	#8214	0.7343	0.7762	0.7762
	#9360	0.3723	0.3333	0.3936

Table 2. PM6 results.

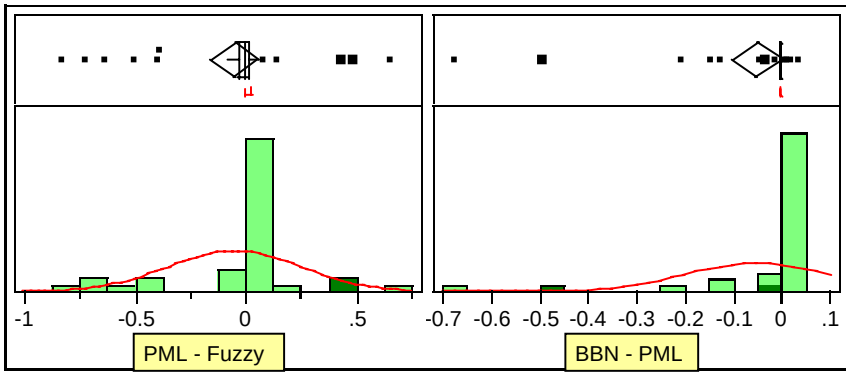
4.2. Estimating Operational State

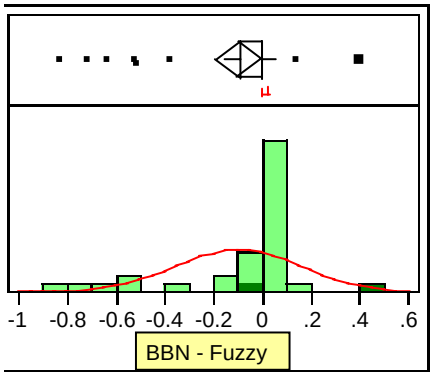
During each simulation, nine performance measures were initially developed to determine the effectiveness of each implementation [11] with respect to various concerns. Of the nine used, two measures are significant for our purposes herein – Performance Measure 4 (PM4) and Performance Measure 6 (PM6). PM4 was a modification of the tuning criteria, measuring how far out of first place (in a ranking of most likely states) the actual operational state is at simulation termination (less is better). PM6 measured the fraction of time the implementation's estimated state *did not* match the enemy's actual state during the entire simulation run (less is better).

A summary of the simulation results are depicted in Tables 1 and 2. Examining PM4 (Table 1), we see all three implementations successfully predicted the actual enemy operational state at termination in thirty-one of thirty-four trials (97% accuracy). Of the three mistaken estimates, all three coordinators ranked the actual operational state second at simulation termination on missions #9026 and #0810, while the Fuzzy coordinator alone correctly identified decisive attack on mission #5412.

The accuracy of PM4 validates our principal research objective, to wit: the meta-model's ability to fuse low-level sensor information into a meaningful and accurate result when our interest is a static prediction of operational state. In this capacity all three of the network inference methods were able to ultimately resolve operational uncertainty by sensing enemy activity alone. Additionally, the consistency in PM4 performance across all three implementations suggests that a strategy of adopting a unifying and implementation-independent quality in the meta-model approach to sensor fusion makes sense. Furthermore, it provides a logical architecture for developing pure information models of military operations. This capability is essential for an accurate understanding of how future forces might leverage information to compensate for reductions in more traditional force-effectiveness dimensions such as pure power and lethality afforded by heavily armored and fitted force.

PM6 provides more information on how the implementations performed throughout the simulation. Here, implementation performance varied greatly among the inference models.





Shapiro-Wilk W Test		Shapiro-Wilk W Test		Shapiro-Wilk W Test	
W	Prob<W	W	Prob<W	W	Prob<W
0.801234	<.0001	0.446877	<.0001	0.721765	<.0001

Figure 10. Shapiro-Wilk goodness-of-fit testing for normality of difference distributions.

Some implementations did well predicting some operational states, while others did not. For example, all implementations successfully predicted the sustainment missions across all mission lifetimes, and performed well throughout the simulation for defense, deliberate attack, and shaping attack as well. However, during retrograde missions, the BBN implementation spent approximately 30% of the simulation time in an incorrect estimation

mode of the actual operational state, while the PML and Fuzzy implementations spent 41% and 72% of the simulation time, respectively, in an incorrect estimation state.

To assess whether the observed differences in PM6 were statistically significant, we turned to a paired testing because the results are linked via individual authors. The assumption of normality on the distribution of computed differences required by both the Student's t-Test and Tukey-Kramer Highest Significant Difference (HSD) was unsupported by the data when examined with both Shapiro-Wilks (Figure 10) and Ryan-Joiner (Figure 11) goodness-of-fit tests.

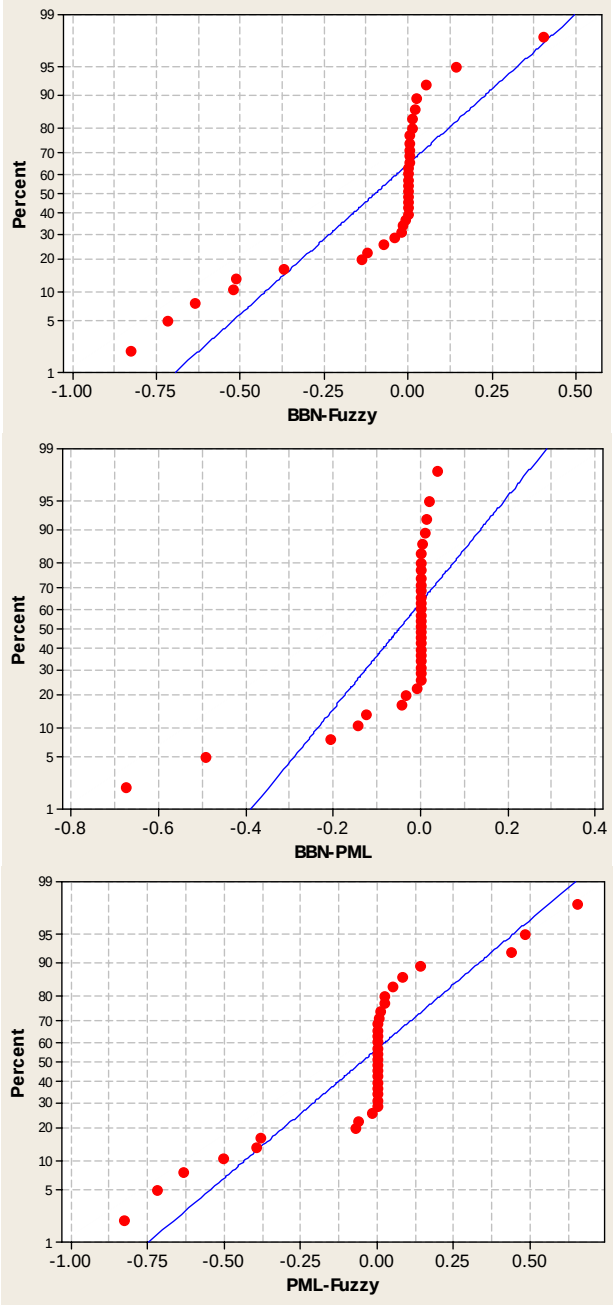


Figure 11. Ryan-Joiner test results for normality of difference distributions: all p-values <0.010.

All Missions	N	n'	W	p-value
BBN – PML	34	13	19.0	0.069
BBN – Fuzzy	34	25	105.0	0.125
PML - Fuzzy	34	24	146.0	0.920
Defense				
BBN – PML	10	1	1.0	1.000
BBN – Fuzzy	10	10	46.0	0.067
PML - Fuzzy	10	10	41.0	0.185
Retrograde				
BBN – PML	7	6	4.0	0.208
BBN – Fuzzy	7	7	0.0	0.022
PML - Fuzzy	7	7	5.0	0.151
Decisive Attack				
BBN – PML	6	3	1.0	0.423
BBN – Fuzzy	6	4	7.0	0.584
PML - Fuzzy	6	4	10.0	0.100
Shaping Attack				
BBN – PML	5	3	1.0	0.423
BBN – Fuzzy	5	4	0.0	0.100
PML - Fuzzy	5	3	2.0	0.789

Table 3. Wilcoxon signed-rank test for differences in median performance on PM6.

We instead used the more robust nonparametric Wilcoxon signed-rank test [30] which does not require the normality assumption. The results in Table 3 support that the differences observed in PM6 are not statistically significant for standard values of significance ($0.01 \leq \alpha \leq 0.1$), although the small sample sizes lead us to conclude this with caution.

In terms of the observable differences on PM6, we believe that culpability for this behavior is attributable to three principle causes. First, while the static criteria of end-state estimation imbedded in the tuning phase implicitly drives each coordinator to achieve a successful prediction of operational state as soon as possible via a minimization, it is inadequate to the task of maintaining a lock onto such a prediction enroute to this state. The

tuning phase for this experimentation adhered to currently accepted conventions [31] by using 25 missions (5 per operational state) to tune the parameters of each coordinator until each of the coordinators successfully estimated the actual operational state at simulation termination. These parameters included the conditional probability values in the Bayesian coordinator, the state transition probabilities in the PML coordinator, and the fuzzy variable membership functions in the Fuzzy coordinator. We then discarded the 25 missions comprising this training set, and used 34 new user-generated missions to assess our meta-model architecture. We made no attempt to measure or control coordinator behavior prior to termination because the issue at-hand concerned assessing the meta-model's capability of accommodating each of the coordinators. In retrospect, this static tuning limits our ability to make maximum use of this architecture. Investigation into appropriate alternative tuning methods that focus on improving inference model performance during the simulation's state transition stages is on-going.

Secondly, the inherent difference in the manner in which each coordinator represents uncertainty induces a natural variability in their comparative performance. The Bayesian coordinator uses a pure mathematical definition of probability as a measure of uncertainty [25]. In the PML coordinator, the rapid growth in the key descriptor state space forced us to abandon probability-based transitions in the face of less mathematical, albeit time proven, certainty factors advocated in the literature [7]. The Fuzzy model uses yet another definition of uncertainty altogether [32]. These differences reflect accepted applications of these frameworks in uncertainty modeling [28]. However, there is an emerging interest [29] in examining the interfaces between phenomena, uncertainty calculi and observers to move away from mutually exclusive approach to imbedded representations. For information fusion within this meta-model architecture, perhaps a hybrid approach of the three inference methods would prove more effective still.

Lastly, we used a different definition of key descriptor values in the Fuzzy model. In the Bayesian and PML models, key descriptor values were calculated as strict binaries (i.e., present or not-present). In the Fuzzy model, each key descriptor was represented as a fuzzy variable. For example, consider KD7, which indicates when the force center is in the southwest quadrant of the simulated battlefield. In the Bayesian and PML models, KD7 was activated when the center was exactly across an imaginary set of grid lines. In the Fuzzy

model, the enemy center could assume varying degrees of "southwestness" as the center approached the same grid lines. Fuzziness at the key descriptor level of the meta-model directly translates into the calculation of the final predicted enemy state fuzzy variable when fuzzy rules are evaluated and combined; as a result, it could account for some of the observed differences in performance overall.

5. Discussion

Existing information fusion techniques, comprised of mostly augmented human systems, are largely *bottom-up* driven, consequently producing localized results with regard to time and space. By this we mean that with the exception of specialized national and theater assets, battlefield information is generally fused along echelons of command and unit size. Each commander analyzes sensor data within his/her purview, and reports an opposing force's activities within the context of their constrained view of the battlefield. The *top-down* manner in which we derive operational states from enemy intent, and key descriptors from operational states allows one to specify exactly how and where low-level sensor information products are combined, thereby reshaping the typical localized filtering process and transcending unit boundaries, locations, and echelons. In this scenario, a satellite image might very well combine with a soldier's report on one side of the battlefield to assemble evidence for a key descriptor. Thus, the meta-model's underlying fusion approach is directly aligned with the type of future battlespace structure envisioned under current force transformation efforts.

Our choice to develop this meta-model architecture with a focus on a single force's behavior increases its applicability for modeling purposes. By creating a modular unit that can be combined with other meta-models, the architecture can be used in pure information-based force-on-force simulations. Moreover, by focusing one meta-model on opposing force operations and a separate one on friendly force operations, a practical operational measure for assessing information advantage results. In the following discussion, we assume that we have applied an alternative tuning method for the parameters of the network learning model as described earlier.

5.1. Information Advantage

Using the meta-model architecture, suppose that we select a particular network inference method, say BBN, for its ability to out-perform the others by having a higher rate of accurately estimating and locking onto the actual operational state of a force in the context of the force's specific battlespace presence in a minimal amount of time. Herein we assumed a conventional force presence in which five force operations defined the suite of possible operational states.[1]

Let $IC_F = \{s_1(v), s_2(v), \ldots, s_f(v)\}$ represent the set of intelligence gathering capabilities for friendly forces, and $IC_O = \{s_1(v), s_2(v), \ldots, s_o(v)\}$ do so for an opposing force (Figure 12). These capabilities are represented directly in each meta-model through the specification and distribution of sensor types (S) and the associated sensor information value mapping functions (V).

Select any pair of potential battlespace force-on-force friendly (O_f) and opposing force (O_O)operational states. Let $\tau^*_{IC_F}(O_O)$ and $\tau^*_{IC_O}(O_f)$ represent the time that each meta-model locks on to its estimate of the actual operational state for opposing forces and friendly forces, respectively. The information asymmetry existing in the battlespace through inference on these operational states is measured by the difference: $\Delta\tau^* = \tau^*_{IC_f}(O_O) - \tau^*_{IC_O}(O_f)$. When $\Delta\tau^* < 0$, information asymmetry exists in favor of friendly forces. The structure of friendly intelligence gathering capabilities provides them with an ability to accurately estimate the opposing force operational state O_O in less time than that required by the opposing force to do the same regarding O_f. Conversely, when $\Delta\tau^* > 0$ information advantage goes to the opposing forces. Parity exists when $\Delta\tau^* \approx 0$.

[1] The meta-model could just as well have used stability or sustainment operations as the focus of inference estimates, decomposing these into sets of key descriptors and adjusting the uncertainty metrics accordingly.

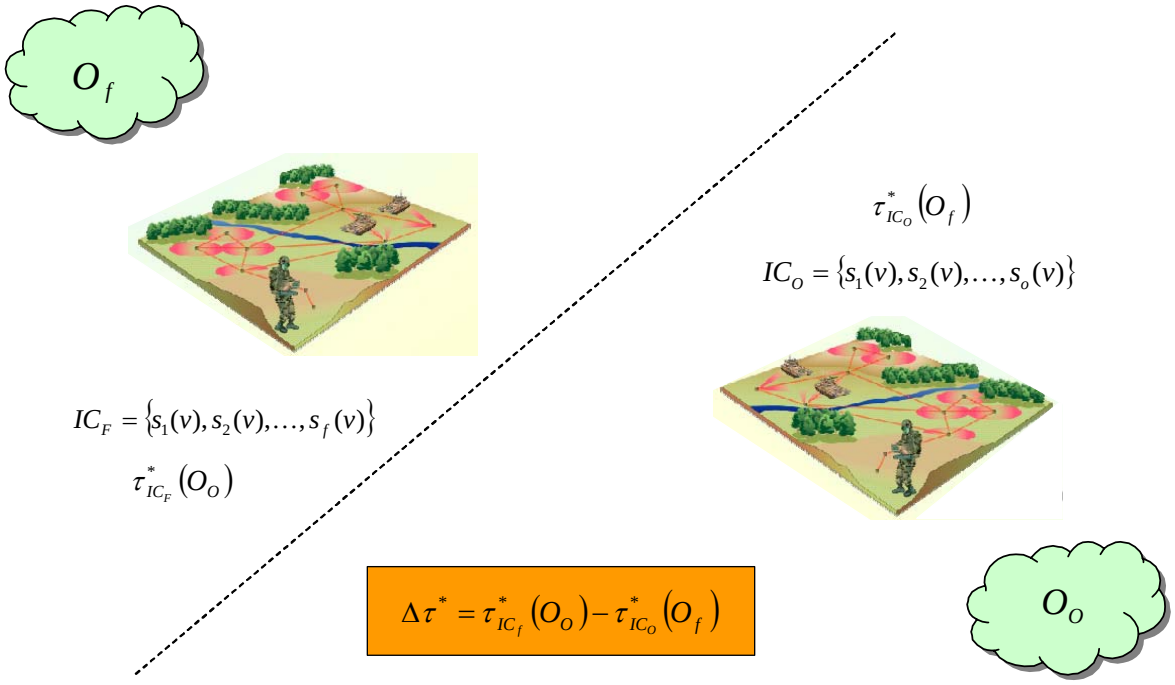


Figure 12. Asymmetric intelligence gathering capabilities.

To assess the overall force capability in this regard, one could apply an aggregate measure across all possible pairs of operational states. However, because this would tend to hide important operational weaknesses, a better approach would be to simply profile the comparison in using a tornado graph or similar display, hypothetically shown in Figure 13. This approach would highlight operational strong and weak points in this regard, illuminate where intelligence capabilities require augmentation, and suggest how one might consider cross-leveling capability to achieve a more globally strategic information advantage for the force.

For the pairwise comparisons of hypothetical friendly operational states (OF*) to opposing force operational states (OO*) shown in Figure 13, we would conclude that the opposing force has a complete information advantage when it is conducting OO3 since the friendly forces at best achieve parity when choosing to conduct OF1 in response. Friendly forces have a strong information advantage against OO2 except for the case when it is paired with OF1.

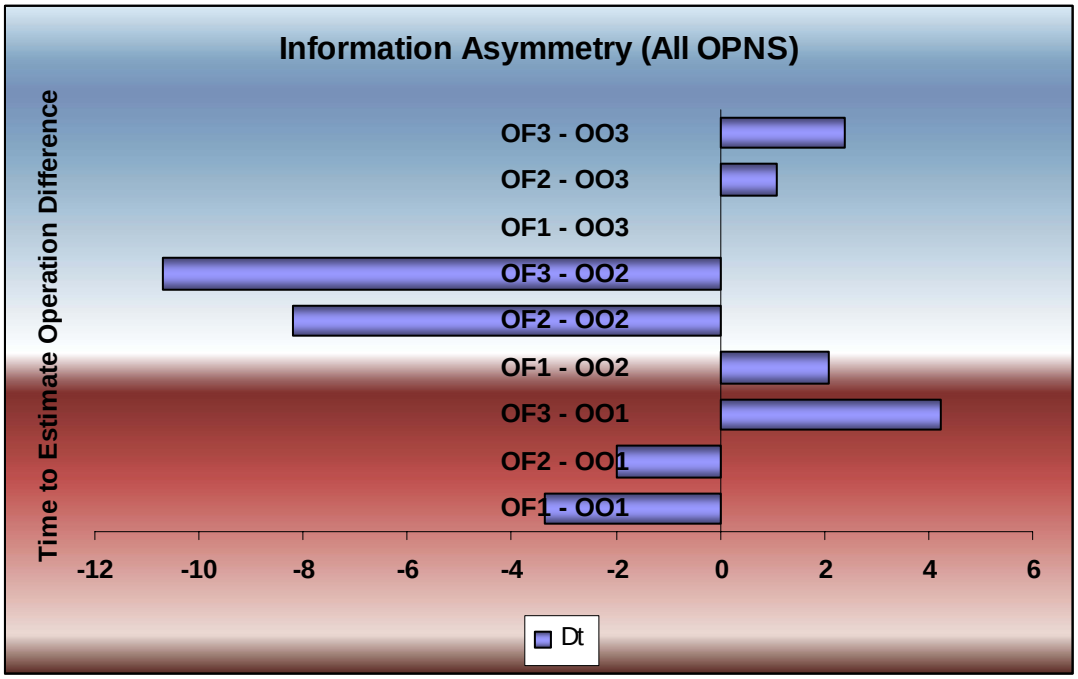


Figure 13. Hypothetical information asymmetry profile of force on force.

In 2 of the 3 missions, $\Delta\tau^*$ indicates that friendly forces should possess an accurate estimate of opposing force operational state much sooner than theirs is known to the enemy. Against OO1, friendly forces again have an information advantage except for the case when OO1 is paired with OF3. The prescription for mitigating the information asymmetry in any one of these pairwise comparisons is to adopt one of the three strategies noted earlier.

We note for completeness that any changes in intelligence capability would necessitate a change in sensor specification along with sensor value functions in the meta-model which, in turn, would induce a response in $\tau^*_{IC_F}(O_O)$ or $\tau^*_{IC_O}(O_f)$ as appropriate.

It is attractive to further consider the opportunity to rank order the effectiveness of proposed changes in capability via a marginal returns assessment, using either improvements in sensor capability: $\partial\tau^*_{IC_F}(O_O)/\partial v_f$, or sensor type: $\partial\tau^*_{IC_F}(O_O)/\partial s_f$. Both quantities are obtainable if one restricts the support for key descriptors to behave monotonically or quasi-monotonically. If the underpinning logic is purely enumerative, this is the case; more is better, or at least more is not worse with respect to levels of support for key descriptors. However, as one incorporates eliminative logic into the structure, the monotonicity of *kd* behavior would depend upon the estimation function as well. And, while imposing

diminishing marginal returns to information gained through the sensor-based system [27], the assessment results in this regard would help systems designers prioritize investment decisions under the usual 'bang-for-the-buck' criteria.

Since an operational state is solely a function of a core minimal set of key descriptors that allows an observing system to distinguish between states, the meta-model architecture provides specific guidance as to how to establish and maintain information advantage: reduce the opposing forces intelligence gathering capabilities (IC_O), maintain and/or increase the span and intensity of friendly intelligence gathering capabilities (IC_F), or *engage in deception operations that create evidence that most effectively support those key descriptors not part of the actual operational state or most effectively contradict evidence supporting the actual operational state*. While the first two options follow directly from the immediately preceding discussion, the latter option is a uniquely enticing aspect of the meta-model. The mapping between observable battlespace actions and operational state key descriptors allows one to couple efficient complementary deception operations to specific friendly force operations with an eye towards minimizing the effectiveness of opposing force inference in a global fashion spanning the entire battlespace. Developing such a strategic deception planning model is not without its challenges, however, and the effectiveness of any deception operation is recognizably dependent upon the ability of the opposing force to receive and process it. This line of reasoning is currently under investigation by the authors.

The meta-model architecture naturally frames the challenge of designing deception operations as a strategic issue in consideration of the specific operational states in existence on the battlefield. Providing evidential support for key descriptors in deception operations is strongly dependent upon the opposing force's ability to receive the signals being sent, regardless of the specific channels selected to provide this mis-information. Potential misinformation supplied to the battlespace by friendly intelligence assets can also be analyzed for effectiveness based on their measurable impact on $\tau^*_{IC_o}(O_f)$.

6. Conclusion

Possessing an accurate estimate of an opposing force's actual operational state provides friendly commanders an ability to shape friendly battlefield activities to disrupt this operational state and hence alter enemy-generated activities as a consequence.

The meta-model architecture we introduce in this study provides a framework within which one can accurately estimate an opposing force's actual operational state in concert with any one of a number of automated network learning systems. This architecture also provides a methodology for determining the degree of information asymmetry between pairs of competing operational states, leading to a suggested methodology for structuring efficient strategic deception operations. Commanders understanding that this information asymmetry is directly linked to evidential support for key descriptors could shape battlefield activities to disrupt the opposing force's operational state. The point we are making here is subtle. We are advocating shifting the battlespace focus from responding to and interdicting enemy *activities* to estimating and disrupting *enemy operational states*, which naturally aligns mission focus at the same conceptual level of abstraction as command intent and thereby directly supports effects-based operations.

A force's operational state can be significantly influenced by a host of complicating factors not considered in this study, such as training, motivation, capability, environmental conditions, and of course its adversary's operational state. Some of these complicating factors, in particular those that have elements that are directly observable by sensor systems, can be accommodated in the meta-model in a straightforward manner by expanding the set of key descriptors accordingly. Others require significant modifications to the meta-model. As an example, for this architecture we implicitly assume that a force's operational state is independent of that chosen by its adversary since there are no looping constructs in the inference chain shown in Figure 1. However, if evolving force interaction is of interest in further work, then this assumption should be avoided so that first and possibly second order feedback behavior is considered in the inference chain as well. One could furthermore incorporate expert opinion into the architecture by applying selective convex weighting coefficients to the individual operational states within the model's estimation functions. Such a preferential weighting could also be applied to the estimation functions themselves using methods specifically designed to aggregate subjective distributions under uncertainty [33].

Fusion systems using the meta-model architecture can define a discrete and minimum set of battlefield sensors and key descriptors that completely differentiate all possible opposing force operational states. To accomplish this, one could adopt a two-stage optimal

matching of available sensors to key descriptors and a matching of key descriptors to operational states in order to reduce the sets of key descriptors used in a meta-model to their minimum size. Possible optimality objectives under such an approach could include minimizing total sensor quantity, minimizing operational state uncertainty, maximizing sensor redundancy, or minimizing ontological overlap [34]. This final objective is the logical analog to maximizing mutual exclusivity between key descriptor sets. One could also consider applying a principle of diminishing marginal returns under constrained time-space considerations in order to identify efficient allocation of sensors [27].

Force designers could easily make use of this information to establish guidelines for sensor survivability, sensor scheduling, and sensor communication networks [26]. Since the meta-model framework is inclusive of any type of sensor including human, mixed-mode and composite suite design is also afforded by the results. Since the meta-model, culling as it does from deployed systems those that have very low marginal contributions to inference, can yield information about how much each sensor contributes to the operational state estimation process, one might use the meta-model architecture as a tool for evaluating an existing sensor organization.

Finally, we note that successfully using this architecture for fusing battlefield information depends on carefully constructing definitions for key descriptors with the goal of capturing a core set of differentiating elements. While our characterization of key descriptors based on FM 3.0 appears sufficient for this study, we suspect that more sophisticated definitions for these descriptors could improve the estimations provided by the inference models, especially for those operational states having less well-defined space and time characteristics, such as a retrograde mission. This option is currently being explored in concert with doctrinal researchers at the US Army War College in concert with the Office of Force Transformation's Transformation Research Program.

7. References

[1] Staats, R. and F.P. Stein. 2003. "Operationalizing network centric warfare," White Paper, MITRE Project 0703D230.

[2] Alberts, D.S., J.J. Garstka, F.P. Stein. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority*, DoD Command and Control Research Program, Washington, DC.

[3] Datta, A., I.R. Viguier. 2000. “Handling sensor data in rapidly changing environments to support soft real-time requirements,” *INFORMS Journal on Computing*, Vol. 12, No. 2, 84-103.
[4] McIntyre, G., K. J. Hintz. 1996. "An information theoretic approach to sensor scheduling," in *Proceedings* 1996 SPIE International Symposium on Aerospace/Defense Sensing & Control, Vol. 2755.
[5] Wand, Y., R. Weber. 2002. “Research commentary: information systems and conceptual modeling – a research agenda,” *Information Systems Research*, Vol. 13, No. 4, 363-376.
[6] Schum, David A. 2001. *The Evidential Foundations of Probabilistic Reasoning*, Northwestern University Press, Evanston, Illinois.
[7] Halpern, Joseph Y. 2003. *Reasoning about Uncertainty*, Massachusetts Institute of Technology, Cambridge, MA.
[8] Pearl, Judea. 1988. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann Publishers, San Francisco, CA.
[9] Beasley, J.E. 1996. *Advances in Linear and Integer Programming*, Oxford University Press, New York, NY.
[10] Ballou, D, R. Wang, H. Pazer, G. Kumar-Tayi. 1998. “Modeling information manufacturing systems to determine information product quality,” *Management Science*, 44(4), 462-484.
[11] Henderson, S.H. 2003. “Intelligent information fusion in battlefield sensor networks,” MS Thesis, Department of Systems & Industrial Engineering, University of Arizona, Tucson, AZ.
[12] Antony, R.T. 1995. *Principles of Data Fusion Automation*, Artech House Books, Norwood, MA.
[13] FM 3-0. Operations.
[14] Francis, Paul L. 2003. *Issues Facing the Army’s Future Combat Systems Program*, United States General Accounting Office report GAO-03-1010R, Washington, DC.
[15] Kolmogorov, A.N. 1956. *Foundations of Probability*, 2nd English Edition, Chelsea Publishing Company, New York, New York.
[16] Technical Panel for C3. 1991. "Data fusion lexicon," U.S. Department of Defense, Data Fusion Subpanel of the Joint Directors of Laboratories.
[17] Poli, R. 2002. “Ontological methodology,” *International Journal of Human-Computer Studies*, Vol. 56, 639 – 664.
[18] Driscoll, P.J., and E. Pohl. 2002. “Modeling the uncertainty of sensor-to-shooter networks,” *Proceedings of the 6th International Conference on Information and Data Quality*, Massachusetts Institute of Technology, Cambridge, Massachusetts.
[19] Geiger, D. and D. Heckerman. 1991. “Knowledge representation and inference in similarity networks and Bayesian multinets,” *Artificial Intelligence*, 82, 45 – 74.
[20] Zadeh, L.A. 1984. “Fuzzy probabilities,” *Information Processing & Management*, 3, 363 – 372.
[21] Huth, M. and M. Ryan. 2000. *Logic in Computer Science: Modeling and Reasoning about Systems*, Cambridge University Press, Cambridge, MA.
[22] Wymore, W. 1993. *Model Based Systems Engineering*, CRC Press, New York.
[23] Cushing, B.E. 1974. “A mathematical approach to the analysis and design of internal control systems,” *Accounting Review*, 49(1), 24 – 41.

[24] Buchanan, B.G., and E.H. Shortliffe. 1984. *Rule-based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*, Addison-Wesley, New York.
[25] Henkind, S., and M. Harrison. 1988. "An analysis of four uncertainty calculi," IEEE Transactions on Systems, Man, and Cybernetics, 18(5), 700 – 714.
[26] Hall, D.L. 1992. *Mathematical Techniques in Multisensor Data Fusio*n, Norwood: Artech House, New York.
[27] Driscoll, P.J., L. Lamm, G. Lamm. 2002. " Networked unattended ground sensor fields – tradeoff study and configuration rules," ORCEN Technical Report DSE-TR-02-10 (DTIC ATA #405461), U.S. Military Academy, West Point, New York.
[28] Parsons, S. 2001. *Quantitative Methods for Reasoning Under Uncertainty*, The MIT Press, Cambridge, Massachusetts.
[29] Zimmerman, H. 1998. "A fresh perspective on uncertainty modeling: uncertainty vs. uncertainty modeling," in *Uncertainty Analysis in Engineering and Sciences: Fuzzy Logic, Statistics and Neural Network Approach*, eds. B.M. Ayyub and M.M. Gupta, International Series in Intelligent Technologies, Kluwer Academic Publishers, Boston, Massachusetts.
[30] Conover, W.J. 1999. *Practical Nonparametric Statistics*, 3rd Edition, John Wiley & Sons, New York.
[31] Ayyub, B.M., and M.M. Gupta. 1997. *Uncertainty Analysis in Engineering and Sciences: Fuzzy Logic, Statistics, and Neural Network Approach*, Kluwer Academic Publishers, Boston, Massachusetts.
[32] De Baets, B. 1997. "A fuzzy morphology: a logical approach," in *Uncertainty Analysis in Engineering and Sciences: Fuzzy Logic, Statistics, and Neural Network Approach*, Kluwer Academic Publishers, Boston, Massachusetts.
[33] Clemen, R.T., and R.L. Winkler. 1999. "Combining probability distributions in risk analysis," *Risk Analysis*, 19 (2), 187 – 203.
[34] Green, P.M. 1996. "An ontological analysis of information systems analysis and design grammars in upper CASE tools," unpublished Ph.D. thesis, The University of Queensland, Australia.
[35] Pidd, M. 2004. *Systems Modelling: Theory and Practic*e, John Wiley & Sons Ltd., Chichester, West Sussex, England.

Distribution List

The list indicates the complete mailing address of the individuals and organizations receiving copies of the report and the number of copies received. Due to the Privacy Act, only use business addresses; no personal home addresses. Distribution lists provide a permanent record of initial distribution. The distribution information will include the following entries:

NAME/AGENCY	ADDRESS	COPIES
Author(s)	Department of Systems Engineering Mahan Hall West Point, NY 10996	2
Client	Office of Force Transformation 1401 Wilson Boulevard, Suite 301 Arlington, VA 22209	1
Dean, USMA	Office of the Dean Building 600 West Point, NY 10996	1
Defense Technical Information Center (DTIC)	ATTN: DTIC-O Defense Technical Information Center 8725 John J. Kingman Rd, Suite 0944 Fort Belvoir, VA 22060-6218	1
Department Head-DSE	Department of Systems Engineering Mahan Hall West Point, NY 10996	1
ORCEN	Department of Systems Engineering Mahan Hall West Point, NY 10996	5
ORCEN Director	Department of Systems Engineering Mahan Hall West Point, NY 10996	1
USMA Library	USMA Library Bldg 757 West Point, NY 10996	1

REPORT DOCUMENTATION PAGE – SF298

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
27-05-2005	Technical Report	June 2004 – May 2005

4. TITLE AND SUBTITLE

A Meta-Model Architecture for Fusing Battlefield Information

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Patrick J. Driscoll, Ph.D.

MAJ Steven J. Henderson, M.S.

5d. PROJECT NUMBER
DSE-R-0517

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Department of Systems Engineering
U.S. Military Academy
Official Mail & Distribution Center
646 Swift Road
West Point, New York 10996

8. PERFORMING ORGANIZATION REPORT NUMBER
DSE-TR-0517

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Force Transformation
1401 Wilson Blvd, Suite 301
Arlington, VA 22209

10. SPONSOR/MONITOR'S ACRONYM(S)
OFT

11. SPONSOR/MONITOR'S REPORT

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A - Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES
None

14. ABSTRACT

The principal contributions of this study are four-fold. First, we propose and illustrate a unifying meta-model architecture for fusing information in sensor-based decision support systems capable of delivering to the user strong inference results in support of tactical decision-making. Second, we demonstrate the feasibility of a completely automated system performing effective estimation of force operational states based on sensor data alone using a new web-based interactive tactical simulation. Third, we show that this architecture can readily accommodate several major network inference methods that are designed to handle battlespace uncertainty. And lastly, we discuss how this approach can be used to directly assess the information advantage of US Forces relative to opposing force intelligence gathering capabilities and the implications of doing so on developing strategic deception operations.

15. SUBJECT TERMS
Wargaming, Information Advantage, Logical ontology

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
unclassified	unclassified	unclassified	None	40	Dr. Pat Driscoll 845-938-6587

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18